IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiffs,

vs. **CR. No. 16-4571 JCH**

GUY ROSENSCHEIN,

Defendant.

MEMORANDUM OPINION AND ORDER

This matter is before the Court on two related motions: The first is the *Motion to Quash Subpoena by New York Times Reporter Gabriel J.X. Dance* [Doc. 249], in which he asks the Court to quash Defendant's subpoena calling him to testify on the hearing on Defendant's motions to suppress evidence. Defendant has filed a response [Doc. 259], and the movant, Mr. Gabriel J.X. Dance ("Dance") has filed a reply. The second is the *United States' Opposed Supplemental Motion to Exclude Defense Witnesses* [Doc. 232], in which the Government asks the Court to exclude Dance's testimony at the hearing. Defendant has filed a response [Doc. 243] to that motion as well. After reviewing the briefs, exhibits, and the relevant legal precedents, the Court concludes that both motions should be granted.

BACKGROUND

Defendant has been charged with nine counts of distribution of child pornography and six counts of possession of child pornography. The Government alleges that the investigation of Rosenschein began when the Bernalillo County Sheriff's Office ("BCSO") received two CyberTipline Reports from the National Center for Missing and Exploited Children ("NCMEC").

The two CyberTipline Reports were generated by Chatstep, an electronic service provider that hosts internet-based conversation between users. In those reports, Chatstep notified NCMEC that images of child pornography were uploaded through its service. In both reports, Chatstep indicated that the user responsible for uploading the images was identified as "Carlo."

Chatstep identified the pornographic images by using PhotoDNA, a cloud-based service developed by Microsoft and available for electronic service providers to help prevent the sharing of harmful images of child exploitation. PhotoDNA works by using a computer algorithm to translate an image into a numerical value that is matched against databases of numerical values generated from images known to be child pornography. Chatstep submitted the contraband images to NCMEC, which then forwarded the material to the New Mexico Attorney General's Office Internet Crimes Against Children ("ICAC") Task Force. Then, BCSO initiated a criminal investigation of Defendant, which resulted in a search of his home and his arrest.

Defendant has moved to suppress evidence, including the images of child pornography that law enforcement officers found in his home. One of Defendant's theories is that when Microsoft developed PhotoDNA and made it available to electronic service providers, it was acting as an agent of the government and for a law enforcement purpose. Therefore, Defendant reasons, when PhotoDNA was used to scan the images he uploaded on Chatstep, that was an unconstitutional search by a government agent. On the other hand, Microsoft witnesses have testified that the company developed PhotoDNA for its own business reasons and not for a law enforcement purpose.

The movant, Dance, is a reporter for the New York Times who co-authored a November 9, 2019 article titled, "Child Abusers Run Rampant as Tech Companies Look the Other Way." The thesis of the article is that technology companies like Amazon, Apple, Facebook, Google, and

Microsoft "have the technical tools to stop the recirculation of abuse imagery by matching newly detected images against databases of the material. Yet the industry does not take full advantage of the tools."[1] With regard to Microsoft specifically, the article describes how the New York Times constructed a computer program that was able to search for and find child pornography using Microsoft's search engine, Bing. According to the article, the authors brought the matter to Microsoft's attention and the company said that it was "re-examining" the issue, with the company's spokesman describing the problem as a "moving target." Yet, later runs of the The Times' computer program found even more child pornography. The article quotes a former Microsoft employee who left the company in 2006 as saying, "it looks like they're not using their own tools" and that the company seemed to be unaware of how its platforms could be manipulated by criminals. Dance discussed the article in a podcast titled "A Criminal Underworld of Child Abuse" on the New York Times' The Daily, February 19-20, 2020.

Defendant asserts that he needs to call Dance to "prove that Microsoft's claim that 'combatting the spreads of child sexual abuse material in the cloud is critical to the protection of Microsoft's brand as a technology company that is worthy of company trust' simply lacks candor." Doc. 259 at 9 (quoting Doc. 82-6 at ¶ 6, Decl. of Jeff Lilleskare)). Defendant contends that he asked the Government to stipulate to Dance's article being introduced as evidence at the suppression hearing, but it would not agree, forcing him to call Dance as a witness.

DISCUSSION

Dance moves to quash the subpoena on two grounds: first, that the reporter's privilege protects him from having to testify involuntarily, and second, that Rule 17 supports quashal

[1] https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html

because his testimony is irrelevant and inadmissible hearsay. The Government moves to quash on the grounds that Dance's testimony is irrelevant and "because the parties are not privy to Mr. Dance's source(s) of information." Doc. 232 at 1.

I. The Reporter's Privilege

Freedom of the press is enshrined in the First Amendment. In *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972), the Supreme Court expressly recognized that a reporter's newsgathering activities qualify for First Amendment protection and noted that its application should be judged by a balancing of interests:

> The asserted claim to privilege should be judged on its facts by the striking of a proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct. The balance of these vital constitutional and Societal interests on a case-by-case basis accords with the tried and traditional way of adjudicating such questions.

Id. at 710.

The reporter's privilege for nonconfidential unpublished information serves the "paramount public interest in the maintenance of a vigorous, aggressive and independent press capable of participating in robust, unfettered debate over controversial matters, an interest which has always been a principal concern of the First Amendment." *Baker v. F & F Inv*., 470 F.2d 778, 782 (2d Cir. 1972). It protects the "pivotal function of reporters to collect information for public dissemination." *Petroleum Prods. Antitrust Litig*., 680 F.2d 5, 8 (2d Cir. 1982). The Second Circuit has explained the reasoning behind the reporter's privilege for nonconfidential information:

> If the parties to any lawsuit were free to subpoena the press at will, it would likely become standard operating procedure for those litigating against an entity that had been the subject of press attention to sift through press files in search of information supporting their claims. The resulting wholesale exposure of press files to litigant scrutiny would burden the press with heavy costs of subpoena compliance, and could otherwise impair its ability to perform its duties—particularly if potential sources were deterred from speaking to the press, or insisted on remaining

> anonymous, because of the likelihood that they would be sucked into litigation. Incentives would also arise for press entities to clean out files containing potentially valuable information lest they incur substantial costs in the event of future subpoenas. And permitting litigants unrestricted, court-enforced access to journalistic resources would risk the symbolic harm of making journalists appear to be an investigative arm of the judicial system, the government, or private parties.

Gonzales v. NBC, Inc., 194 F.3d 29, 35 (2d Cir. 1998).

Defendant argues that the privilege does not apply in this case because he does not intend to ask Dance to reveal the names of his sources. However, as other courts in the Tenth Circuit have recognized, the newsperson's privilege protects both confidential and non-confidential *information* and sources. *See e.g., In re Bacon for an Order Pursuant to 28 U.S.C. § 1782 to Conduct Discovery for Use in Foreign Proceedings v. Archer*, 17-mc-00192-KLM, 2018 WL 4467182, at *4 (D. Colo. Sept. 17, 2018) (unpublished) (rejecting the argument that privilege does not apply merely because party issuing subpoena was not seeking to identify confidential sources); *United States v. Foote*, No. 00-CR-20091-01-KHV, 2002 WL 1822407, at *2 (D. Kan. Aug. 8, 2002) (unpublished) ("[N]onconfidential information gathered by a reporter or other journalist is entitled to privilege as well"); *Re/Max Int'l., Inc. v. Century 21 Real Estate Corp*., 846 F. Supp. 910, 911 (D. Colo. 1994) (quoting *Loadholtz v. Fields*, 389 F. Supp. 1299, 1302-03 (M.D. Fla. 1975) ("This distinction [between confidential and nonconfidential sources] is utterly irrelevant to the 'chilling effect' that ... subpoenas would have on the flow of information ...."). This Court agrees with the reasoning in these cases—the fact that Defendant will not ask Dance to reveal confidential sources but rather non-confidential information does not bar the application of the privilege.

The Tenth Circuit set forth a balancing process by which courts must evaluate a journalist's First Amendment privilege. *Silkwood v. Kerr-McGee Corp*., 563 F.2d 433 (10th Cir. 1977) (citing

Branzburg). The *Silkwood* court established the following elements to be considered in the balance: 1) the nature of the evidence sought; 2) the effort to obtain the information from other sources; 3) the necessity of the information to the requesting party; and 4) the relevance of the information to the matter. *Id*. at 438 (citing *Garland v. Torre*, 259 F.2d 545 (2d Cir. 1958)).

A. Nature of the Evidence Sought

In his affidavit, Dance asserts that he has no personal knowledge regarding Microsoft's business strategy or its motivation for using PhotoDNA. Doc. 249-1 at ¶ 9. Defendant does not dispute either assertion. Rather, he argues that he has subpoenaed Dance to testify regarding the content of his article on the failure of the technology industry generally, and Microsoft specifically, to use available technological tools to effectively root out child pornography on their platforms. Defendant contends that he "just needs to have Mr. Dance verify his reporting is accurate—that Microsoft is not using PhotoDNA on its own cloud services like OneDrive and Azure." Doc. 259 at 4. Defendant does not identify any testimony that he intends to elicit from Dance that falls outside the scope of the news article; he merely wishes to have Dance repeat and verify the contents.

Some of this information, such as statements from current and former employees of Microsoft, is hearsay (which does not necessarily bar its use at a suppression hearing, where the Rules of Evidence do not apply). Other parts, such as the results of tests run by The Times via computer program, may not be. Defendant offers all of this evidence to impeach any Microsoft witness who testifies that Microsoft designed and implemented PhotoDNA to advance its own business purposes rather than for a law enforcement purpose. According to Defendant, evidence showing that Microsoft uses PhotoDNA to scan images on some products like its Bing internet browser but not to scan images that are uploaded to its OneDrive and Azure cloud storage

platforms undermines its position that it uses PhotoDNA to "block[] illegal images of child sexual abuse from its services and the cloud ecosystem" to further its business interests. Doc. 259 at 5 (citing Doc. 82-6 at ¶ 5)).

Although Defendant describes the strength of this impeachment evidence as "gargantuan," the Court agrees with Dance that it is weak. The evidence shows uneven use of PhotoDNA, but it says little about *why* Microsoft designed and uses PhotoDNA in the first place. The evidence in Dance's article shows that Microsoft is not using PhotoDNA on all of its online platforms or with the greatest efficacy or uniformity. But that evidence does not go very far in demonstrating that Microsoft did not implement PhotoDNA for its own business purposes, or for that matter, in showing that the company intended to help law enforcement catch pedophiles. Although Defendant contends that this evidence shows that Microsoft is not using PhotoDNA for its own business purposes, one could just as easily argue the opposite—that it shows Microsoft never intended to use PhotoDNA to help law enforcement, because if Microsoft had that intention it would be using it more diligently across all of its platforms. Alternatively, on could infer that it suits Microsoft's business purposes both to use PhotoDNA with Bing, and at the same time satisfy its customers' demands for privacy by not using it on OneDrive and Azure. Because the evidence is so limited, neither argument is more persuasive than the other. This demonstrates the weakness of Dance's testimony as impeachment evidence.

B. Effort to Obtain the Information from Other Sources

Defendant argues that he has made efforts to obtain other evidence to support his claim that Microsoft does not use PhotoDNA for its own business purposes. Specifically, he cites a discovery request he propounded to the Government asking it to compile a list of other criminal prosecutions the began as a result of a Microsoft customer uploading an image of child

pornography to its OneDrive and Azure platforms.[2] He also notes that it is unfair to expect him to gather the evidence he needs from Microsoft or its employees, as they will deny that the company uses PhotoDNA to further a law enforcement purpose.

It is true that witnesses are typically loath to contradict themselves, and that it is often very difficult to disprove a person's or company's stated intent for its actions. However, the Court cannot conclude that Defendant has gone to great lengths to obtain the impeachment evidence he seeks.

C. Necessity of the Information

Because Microsoft witnesses have testified that the company designed and implemented PhotoDNA for its own business purposes, Defendant clearly needs to impeach them on that point. Otherwise, it will be very difficult for him to demonstrate that the evidence against him should be suppressed because Microsoft was a government agent carrying out an illegal search of his online activities. However, as explained above, it is impossible to consider this evidence to be necessary when it does not actually achieve its impeachment purpose.

D. Relevance to the Case

The question of whether Microsoft designed, implemented, and distributed PhotoDNA for its own business purposes or in order to help law enforcement prevent the online distribution of child pornography is central to the question of whether Microsoft acted as an agent of the Government. However, as explained above, Dance's testimony sheds little light on that question.

E. Conclusion

[2] The Court denied Defendant's motion to compel as to this discovery request in a Memorandum Opinion and Order entered July 15, 2020. [Doc. 281]

The Court concludes that Dance is entitled to the reporter's privilege in this case. Dance has no personal knowledge as to whether or not Microsoft uses PhotoDNA for its own business purposes. He has no testimony to add beyond what is already laid out in his New York Times article—which is presumably why Defendant issued the subpoena only after the Government refused to stipulate to the admission of the article as an exhibit at the hearing. Defendant offers no reason to believe that Microsoft will dispute Dance's assertion in the article that PhotoDNA does not catch all child pornography identified through Bing or that it does not use PhotoDNA on its Azure and OneDrive cloud services. And yet that evidence does not go very far in showing that Microsoft uses PhotoDNA for the purpose of assisting law enforcement and is therefore a government agent. Thus, it is not particularly relevant to the impeachment purpose for which Defendant intends to offer it.

On balance, the *Silkwood* factors weigh in favor of applying the reporter's privilege and quashing the subpoena.

II. Rule 17

Federal Rule of Criminal Procedure 17(a) governs subpoenas *ad testificandum* in criminal proceedings. Rule 17(a) requires that testimony to be both relevant and material. *Stern v. U.S. Dist. Court for the Dist. Of Mass*., 214 F.3d 4, 17 (1st Cir. 2000). As the party who served the subpoena, the burden to make that showing falls to Defendant. *See U.S. v. Nixon*, 418 U.S. 683, 698-699 (1974). Defendant has not shown Mr. Dance's testimony to meet either criterion. Defendant argues that a "criminal defendant must be allowed to test the adverse witness's credibility, including their possible biases, prejudices or motives." Doc. 259 at 6. However, Dance's article, podcast and Declaration demonstrate that he has no knowledge as to Microsoft's biases, prejudices or motives.

Defendant's claim that Mr. Dance's testimony is material and relevant rests on two assertions: "Mr. Dance knows that Microsoft does not run PhotoDNA on Microsoft's OneDrive and Azure systems" and "that Microsoft has been rather lazy, if not cavalier, in its programming of the Bing search engine's capacity to eliminate child pornography from what a user can find on the Internet." Doc. 259 at 7. As already discussed above, neither of these sheds light on whether or not Microsoft developed and implemented PhotoDNA to serve a business purpose or a law enforcement purpose. Therefore, it is neither relevant nor material to the issues at the suppression hearing and should be quashed pursuant to Rule 17.

IT IS THEREFORE ORDERED that the *Motion to Quash Subpoena by New York Times Reporter Gabriel J.X. Dance* [Doc. 249] is **GRANTED**, and the *United States' Opposed Supplemental Motion to Exclude Defense Witnesses* [Doc. 232] is **GRANTED**.

UNITED STATES DISTRICT JUDGE